SPYWOLF

Security Audit Report

Completed on

May 15, 2023

OVERVIEW

This audit has been prepared for **Muskman INU** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Muskman INU

PROJECT DESCRIPTION

According to their whitepaper:

Muskman approaches the creation of our community from a unique perspective. We believe that through the power of collective decentralization, we can build something stronger than a centralized team ever could. A community-run token is nothink without the united individuals who give it purpose. From the early days of Muskman, we will be known as the Muskman Army, both amongst ourselves and across countless other platforms.

Release Date: Presale starts in May, 2023

Category: Meme token

CONTRACT INFO

Token Name	Symbol
Muskman Inu	MMAN

Contract Address
0x3981C8Fe0E9ab8c7E18f1946b805ed03976f8fDF

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
May 13, 2023	Yes

Total Supply	Status
100,000,000,000,000,000	Not launched

TAXES

Buy Tax
none

Sell Tax
5%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	4
Uniq Senders	2
Uniq Receivers	2
Total Amount	150000000000000000 MMAN
Median Transfer Amount	45000000000000000 MMAN
Average Transfer Amount	37500000000000000 MMAN
First transfer date	2023-05-13
Last transfer date	2023-05-13
Days token transferred	1

SMART CONTRACT STATS

Calls Count	4
External calls	4
Internal calls	0
Transactions count	4
Uniq Callers	1
Days contract called	1
Last transaction time	2023-05-13 12:25:24 UTC
Created	2023-05-13 11:54:39 UTC
Create TX	0x0141927ce529c79d43b979a5dfc8baea96f195ad459027d89be95d4a8ecc4397
Creator	0x15649aa701da8c1de88f009412dcdb5cf0698947

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can set buy/sell fees up to 100%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setTaxes(uint256 _rfi, uint256 _marketing,
uint256 _trust, uint256 _liquidity) public onlyOwner {
    taxes.rfi = _rfi;
    taxes.marketing = _marketing;
    taxes.trust = _trust;
    taxes.liquidity = _liquidity;
    emit FeesChanged();
}

function setSellTaxes(uint256 _rfi, uint256 _marketing,
uint256 _trust, uint256 _liquidity) public onlyOwner {
    sellTaxes.rfi = _rfi;
    sellTaxes.marketing = _marketing;
    sellTaxes.trust = _trust;
    sellTaxes.liquidity = _liquidity;
    emit FeesChanged();
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees **combined** not to exceed 25%.

FOUND THREATS

⚠ High Risk

Owner can set max buy/sell/transfer transaction without limitation.
If set to 0 buy/sell/transfer will fail.
When transaction limitations are applied, users will be subject to transfer restrictions to certain amounts (depending ot current setting).

```
function updateMaxWalletBalance(uint256 amount) external onlyOwner {
    maxWalletBalance = amount * 10**_decimals;
}

function updatMaxBuyAmt(uint256 amount) external onlyOwner {
    maxBuyAmount = amount * 10**_decimals;
}

function updatMaxSellAmt(uint256 amount) external onlyOwner {
    maxSellAmount = amount * 10**_decimals;
}
```

- Recommendation:
  - Considered as good transaction limitation is max transaction to be always above 0.1% of total supply.

FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell.
If the liquidity pair is blacklisted, trading will fail for all users.

```
function setAntibot(address account, bool state) external onlyOwner {
    require(_isBot[account] != state, 'Value already set');
    _isBot[account] = state;
}

function bulkAntiBot(address[] memory accounts, bool state) external onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++){
        _isBot[accounts[i]] = state;
    }
}

function _transfer(address from, address to, uint256 amount) private {
..............
require(!_isBot[from] && !_isBot[to], "You are a bot");
..............
}
```

- Recommendation:
  - Considered as good bot protection practice is that it is automated and liquidity pair is always excluded from such restrictions.

FOUND THREATS

⚠ High Risk

If sell taxes are set to 0, once swapTokensAtAmount is reached, contract will halt and selling will fail for all users.
Division by zero is impossible.

```
function setSellTaxes(uint256 _rfi, uint256 _marketing,
uint256 _trust, uint256 _liquidity) public onlyOwner {
    sellTaxes.rfi = _rfi;
    sellTaxes.marketing = _marketing;
    sellTaxes.trust = _trust;
    sellTaxes.liquidity = _liquidity;
    emit FeesChanged();
}

function _transfer(address from, address to, uint256 amount) private {
...................
bool canSwap = balanceOf(address(this)) >= swapTokensAtAmount;
if(!swapping && swapEnabled && canSwap && from != pair && !_isExcludedFromFee[from] && !_isExcludedFromFee[to]){
    swapAndLiquify(swapTokensAtAmount);
}
...................
}

function swapAndLiquify(uint256 tokens) private lockTheSwap{
// Split the contract balance into halves
uint256 denominator = (sellTaxes.liquidity + sellTaxes.marketing + sellTaxes.trust) * 2;
uint256 tokensToAddLiquidityWith = tokens * sellTaxes.liquidity / denominator;
...................
}
```

- Recommendation:
  - Ensure that sell taxes are always above 0 or use another formula in the swapAndLiquify() method.

FOUND THREATS

⚠ Medium Risk

Owner can change autoswap settings.
If autoswap is enabled, swapTokensAtAmount is set to 0, contract will halt and selling will fail.

```
function updateSwapEnabled(bool _enabled) external onlyOwner {
    swapEnabled = _enabled;
}

function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    swapTokensAtAmount = amount * 10**_decimals;
}

function _transfer(address from, address to, uint256 amount) private {
.................
bool canSwap = balanceOf(address(this)) >= swapTokensAtAmount;
if(!swapping && swapEnabled && canSwap && from != pair
&& !_isExcludedFromFee[from] && !_isExcludedFromFee[to]){
    swapAndLiquify(swapTokensAtAmount);
}
.................
}
```

Informational

Owner can exclude address from reflection rewards.

```
function excludeFromReward(address account) public onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}
```

Owner can exclude address from fees, max transaction limit and max wallet restrictions.

When address is excluded from fees and transaction limitations, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function _transfer(address from, address to, uint256 amount) private {
.................
if(!_isExcludedFromFee[from] && !_isExcludedFromFee[to] && !swapping){
    if(from == pair){
        require(amount <= maxBuyAmount, "You are exceeding maxBuyAmount");
    }
    if(to == pair){
        require(amount <= maxSellAmount, "You are exceeding maxSellAmount");
    }
    if(to != pair){
        require(balanceOf(to) + amount <= maxWalletBalance, "You are exceeding maxWalletBalance");
    }
}
.................
}
```

Informational

Owner can set buy/sell fees up to 1% and bonus sell fee up to 10%. Combined buy+sell = 12%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
uint256 constant public maxBuyTaxes = 100;
uint256 constant public maxSellTaxes = 100;
uint256 constant masterTaxDivisor = 10000;

function setTaxes(uint16 buyFee, uint16 sellFee, uint16 bonusSellFee) external onlyOwner {
    require(!taxesAreLocked, "Taxes are locked.");
    require(buyFee <= maxBuyTaxes
            && sellFee <= maxSellTaxes,
            "Cannot exceed maximums.");
    require(bonusSellFee <= 1000, "Cannot exceed 10%.");
    _taxRates.buyFee = buyFee;
    _taxRates.sellFee = sellFee;
    _taxRates.bonusSellFee = bonusSellFee;
}
```

Owner can exclude address from fees, max transaction and max wallet limits. Such limits won't apply on excluded addresses.

```
function setExcludedFromFees(address account, bool enabled) public onlyOwner {
    _isExcludedFromFees[account] = enabled;
}
```

Informational

Owner can withdraw any tokens from the contract with exception of MMAN token.
When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function rescueBNB(uint256 weiAmount) external onlyOwner {
    require(address(this).balance >= weiAmount, "insufficient BNB balance");
    payable(msg.sender).transfer(weiAmount);
}

function rescueAnyBEP20Tokens(address _tokenAddr, address _to, uint _amount) public onlyOwner {
    require(_tokenAddr != address(this), "Cannot transfer out MMAN!");
    IERC20(_tokenAddr).transfer(_to, _amount);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Muskman INU

GOOD PRACTICES FOUND

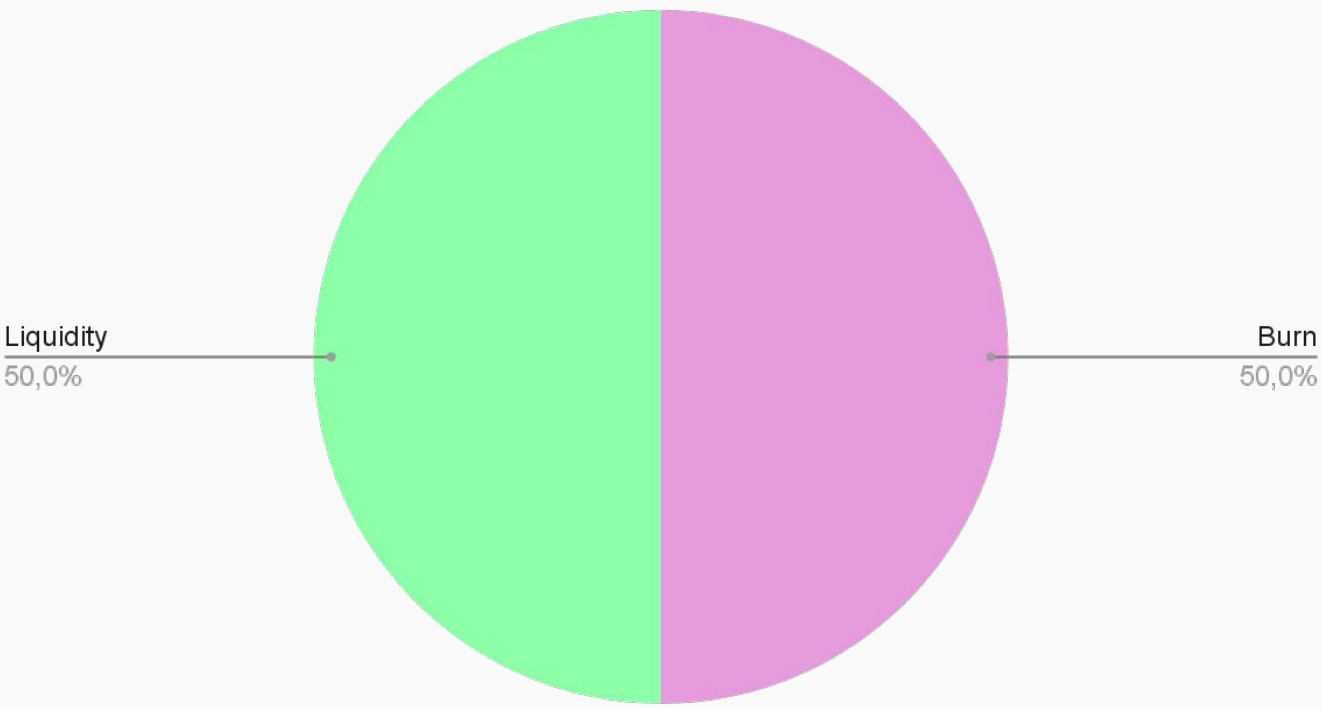
- ✔ The owner cannot mint new tokens after deployment

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 50% - Fairlaunch and Liquidity
- 50% - Burned

Tokens distribution



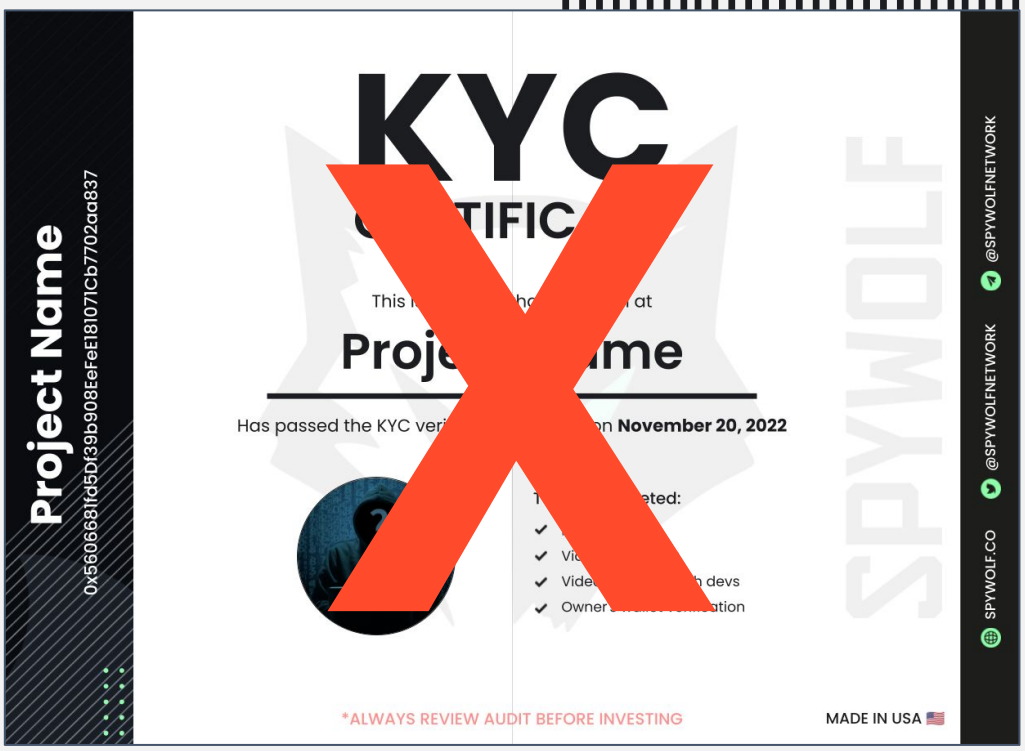
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://muskman.org/

Domain Registry
https://www.namecheap.com

Domain Expiration
2024-04-14

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written , explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

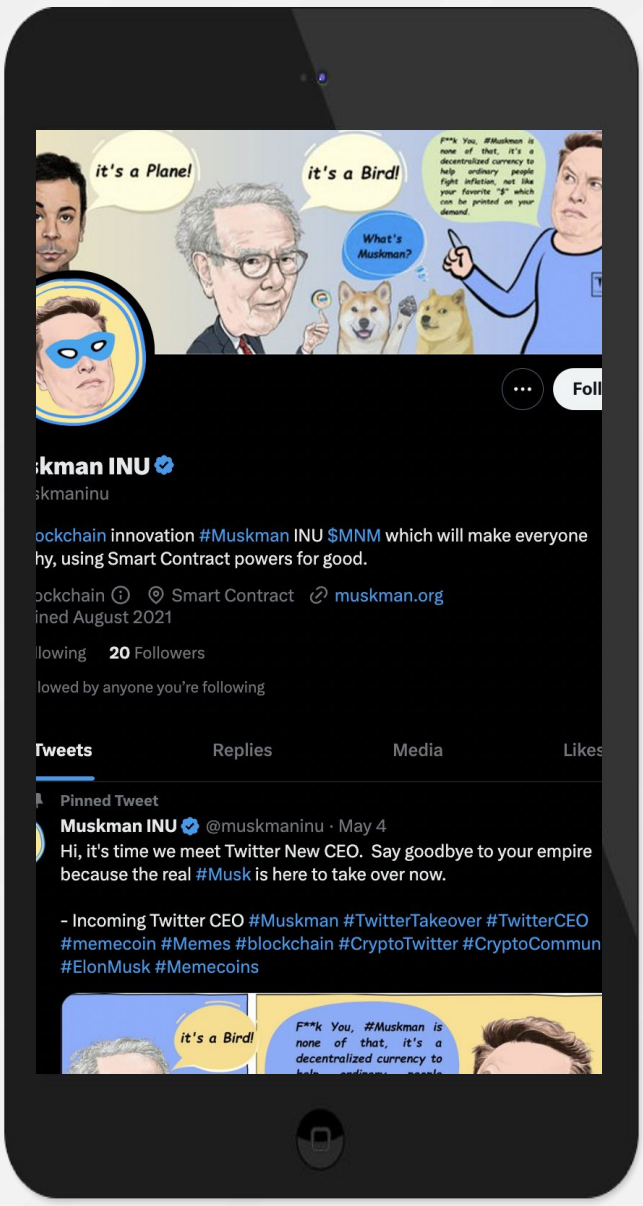
muskman.org

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Some of the project's social media pages are new but active.



Twitter

@muskmaninu

- 1 281 followers
- Active
- Posts frequently

Discord

- Not available

Telegram

@muskmanofficial

- 1 495 members
- Few active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.